Fall 1983

Policy Review

Number 26

Policy Review articles are regularly abstracted or indexed in the leading social science indexing services, including *ABC-Pol Sci, Cumulative Index to Periodicals, Current Contents/Social & Behavioral Sciences, Human Resources Abstracts, International Political Science Abstracts, The Journal of Economic Literature, Monthly Periodical Index, Public Affairs Information Service, Public Studies Documents, Sage Public Administration Abstracts, Sage Urban Studies Abstracts, Social Sciences Citation Index, United Nations Current Bibliographic Information, United States Political Science Documents, and Urban Affairs Abstracts.*

POLICY REVIEW Fall 1983 No. 26

Can Democracy Keep Secrets?

Do We Need an Official Secrets Act?

Guenter Lewy

Under current American law, an employee of the Department of Agriculture who reveals information on next year's soybean crop estimate may find himself behind bars. But an employee of the Defense Department who leaks classified defense information to a member of the press is probably not guilty of any criminal offense. Similarly, a reporter who obtains secret national security information and publishes it on the front page of his newspaper most likely has not committed espionage or violated any law.

The United States may be the only nation . . . without any meaningful defense against the publication of classified defense information.

The qualifications "probably" and "most likely" are necessary because the only certainty about our statutes on leaking and publishing defense information is that they are a morass. Concerned citizens and various commissions of experts have drawn attention to this state of affairs, but Congress has failed to act. The most recent attempt to deal with this charged issue came during the almost decade-long endeavor to update the federal criminal code, but it ended in the spring of 1982 in yet another stalemate between liberals and conservatives. The decision of the Supreme Court in the Pentagon Papers case, which might have clarified some of the constitutional issues involved, instead raised more questions than it answered.

Today the United States may be the only nation in the world without any meaningful defense against the publication of classified defense information. Even in Sweden, a country with a tradition of open government more than two centuries old, a civil servant and two journalists were sent to jail in 1973 for their share in the publication of a series of articles about Sweden's security services. Great Britain, the longest-functioning parliamentary democracy, has one of the strictest systems of official secrecy. On grounds of historical experience, at least, there is therefore room for the argument that the United States could take measures to protect its vital secrets without sacrificing its liberties. Absolutist interpretations of the Constitution, according to which the First Amendment stands in the way of such legislation, deserve a respectful hearing but may prove unconvincing. An unrestricted right to disseminate national security information is not essential for a free people and indeed may threaten the very survival of that society. The Constitution, as the Supreme Court has often affirmed, is not a suicide pact.

Present statutes fall into two categories: those concerning classical espionage, the transmission of defense information to a foreign power; and those governing the disclosure of classified information by a present or former employee or official of the government. As complex and confused as much of this body of law is, it becomes a veritable minefield of legal ambiguities when applied to the publication of such information by the media.

The law concerning espionage is to be found in sections 793 to 798 of Title 18 of the United States Code. Most of these provisions were enacted in the Espionage Act of 1917,[1] and a few were added by the Internal Security Act of 1950.[2] Analysis of the language of these statutes and of their legislative history makes it likely that they do not prohibit the publication of defense information.

The most comprehensive provisions are in section 794. Subsection 794(a) punishes by death or imprisonment up to life the actual or attempted communication to any foreign government or foreign citizen of "any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense." Such communication is unlawful if done "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation." There are ample grounds to think that this section does not aim at public speech or publication. The proscribed activity is communication *to* a foreign recipient; one who publishes defense information does not thereby communicate it to foreigners in the sense of the statute, nor does he necessarily have a culpable intent to injure the United States or aid a foreign power. Presumably, the framers of this legislation saw a difference between communicating and publishing, and an examination of the prolonged debates in the Congress in 1917, covering more than 300 pages of the *Congressional Record*, reinforces, if not confirms, this conclusion.[3]

Subsection 794(b) punishes by death or imprisonment up to life the communication or publication "in time of war" of information concerning the movement or disposition of troops, of plans of military operations or

GUENTER LEWY, *author of* The Federal Loyalty-Security Program: The Need for Reform *(1983), is a professor at the University of Massachusetts.*

fortifications, or of "any other information relating to the public defense, which might be useful to the enemy." Subsection 794(b) is applicable only "in time of war"; however, it punishes not only the communication of defense information to an enemy but also the publication of such information—if done "with intent that the same be communicated to the enemy."

Treasonable Intent

The legislative history of subsection 794(b) reveals that a majority of the Congress in 1917 did not want to prohibit all publication of defense information. Although the Wilson administration sought just such a statute—a blanket restriction on the publication of defense information without any limiting requirement of intent—Senate progressives, including Borah, La Follette, Norris, and Hiram Johnson, feared the aggrandizement of presidential power during wartime and were determined to prevent a general censorship provision. The language that was finally approved therefore required an intent that will be present only very rarely. The only publication prohibited by subsection 794(b) is publication that has the purpose of informing the enemy—the kind of activity engaged in by a disloyal newspaper or by a disloyal person inserting a coded advertisement. Congressional supporters of a more sweeping provision pointed out in the spirited debate that a newspaper's disclosure of defense information could aid the enemy even if the newspaper's editors and reporters acted without a treasonable purpose. Nevertheless, their argument did not prevail, and subsection 794(b) probably reaches only the kind of publication that has the specific purpose of informing the enemy.[4]

Subsection 794(b) harbors other ambiguities. The statute does not say who determines the country's "enemy." And in today's world it is not always obvious who the enemy is. Were the Vietcong who shot at U.S. military advisers in 1964 an enemy within the meaning of the statute, or did they become an enemy only after the introduction of regular U.S. combat forces and the beginning of all-out hostilities with North Vietnam in 1965? In 1972 the United States bombed Chinese ships in Haiphong harbor while it played host to the same country's Ping-Pong team. Was Communist China then our enemy? A statute that exposes the average citizen to such uncertainties in deciding the outer limits of legal activity may have difficulty passing constitutional muster.

Additional problems of interpretation arise with section 793, which names six offenses involving the gathering of defense information, each punishable with imprisonment of up to ten years. Subsection 793(a) covers entering or flying over a defense installation "for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation." Subsection 793(b) concerns taking or copying "with like intent or reason to believe" documents, plans, maps, or photographs from such installations. These offenses are not defined in terms of the actor's intent to deliver defense information to a foreign power, as in subsection 794(a), or to aid an enemy in time of war, as in subsection 794(b). Could these provisions reach the information-gathering activities of reporters or their informants?

There is first the question of the meaning of "information respecting the national defense." In an era when virtually every facet of civilian life can have an important bearing on the nation's military capabilities, what kind of information is included or excluded by that phrase?

The problems of interpretation were noted during the congressional debate in 1917, but no agreement was reached on a more precise term. In the years since, the courts have had occasion to give content to the amorphous language of the statute. In the landmark case of *Gorin v. United States*,[5] decided in 1941, the Supreme Court ruled that the term "information related to the national defense" was sufficiently precise and did not create due-process problems of vagueness. National defense, said the Court, is a "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness." Whether any particular information was related to the national defense and protected by the espionage act was for the jury to determine from an examination of the material and expert testimony on its significance.[6]

The Supreme Court's ruling in the *Gorin* case leaves many questions unanswered. What about information relating to the nation's economic strength, civilian morale, or the diplomatic establishment? How important must the information be? Is every little detail, such as that sailor John Doe has joined the submarine fleet, to be protected? What about information that the government has not sought to keep secret or data that have found their way into the public domain despite such endeavors?

Lawful Sifting

The last-mentioned issue arose in *United States v. Heine*,[7] a case decided in 1945 by Judge Learned Hand of the Court of Appeals of the Second Circuit in a ruling left standing by the Supreme Court. Shortly before World War II, defendant Heine, a naturalized citizen of German origin, had compiled extensive reports on the U.S. aviation industry and had mailed these to different addresses for forwarding to Germany. The evidence allowed the inference that he had chosen this procedure to avoid detection. Still, Judge Hand ruled that Heine was not guilty of espionage because the information Heine collected came from sources that were lawfully accessible to anyone willing to take the pains to find and sift them—books, magazines, newspapers, correspondence with manufacturers, talks with employees. Moreover, the government had not tried to prevent the dissemination of this kind of information. No matter what the motive, Judge Hand concluded, whatever was lawful to broadcast throughout the country was lawful to send abroad.

In the *Gorin* case the expansive reach of the term "national defense" was saved from the constitutional infirmity of overbreadth by Judge Hand's ruling that the sanctions of the act applied only if *scienter* (a knowing violation of the law or a guilty intent) was established: "The obvious delimiting words in the statute are those requiring 'intent or reason to believe that the information

to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.' This requires those prosecuted to have acted in bad faith."[8] The same culpability standard is used in section 794(a) and in other parts of section 793. Applied literally, this way of establishing the presence of *mens rea* (a guilty mind) would appear to create serious difficulties for public speech and publication.

According to the usual meaning of words, a reporter who obtains and publishes secret defense information probably has reason to believe that this information would be used to injure the United States or help a foreign power. Foreigners, and especially agents of foreign intelligence services, are known to be avid readers of our publications. For example, had the *New York Times* in 1961 published an account of the imminent invasion of Cuba, as President Kennedy is said to have thought it should have done, Cuba would undoubtedly have benefited. Read in this way, subsections 793(a) and 793(b) bring about the kind of general prohibition on publication that the Congress in 1917 clearly wished to avoid.

Foreigners, and especially agents of foreign intelligence services, are known to be avid readers of our publications.

Both the House and the Senate were aware of the possible pitfalls in this section of the law. Yet despite the sweeping language of the culpability standard adopted—"intent or reason to believe"—they appear to have been convinced that the information-gathering offenses of subsections 793(a) and 793(b) were adequately limited by a requirement that there exist a proven evil purpose to reveal the information to a foreign country or to injure the United States. If correct, such a reading of the law may indeed protect journalists whose primary purpose in gathering defense information is neither to injure their country nor to aid a foreign nation, but it causes problems in certain traditional cases of espionage. For example, a serviceman who sells military secrets to a foreign agent could claim that his main purpose was to obtain money, not to injure the United States. To prevent such an interpretation, it probably is necessary to focus on the actor's state of mind about the use of the secret information. This would require us to read the phrase "reason to believe" not simply as being aware of likely consequences but as understanding the primary use to which the information will be put by others. The greedy serviceman presumably has reason to believe that the information he sells will be used primarily to injure the United States or advantage a foreign country. By contrast, the reporter is aware that some persons will put his story to such use, but the primary uses he seeks are those that enlighten his compatriots.[9]

Sections 793(d) and 793(e), probably the most confusing of the espionage statutes, come closest to touching the activities of reporters because their sweeping provisions lack a specific evil intent requirement. In the original version this part of the 1917 statute was meant to apply only to government employees. That such employees can be held to a higher standard of loyalty than the population at large may explain the absence of a clear culpability standard. In 1950, while working on the Internal Security Act, Congress split the section into two and made it apply to all persons.

Subsection 793(d) imposes a fine of not more than $10,000 or imprisonment up to ten years on any person who, having lawful access to or possession of any document, map, photograph, etc. "relating to the national defense" or entrusted with information "the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation," willfully communicates the same "to any person not entitled to receive it" or retains the same. Subsection 793(e) imposes the same penalties on anyone who, having unauthorized access to or possession of such items, communicates these to any person not entitled to receive them or willfully retains them. Subsection 793(d) reaches people with lawful possession of defense-related material; subsection 793(e) covers people not connected with the government who have unauthorized possession. Applied literally, these sections could well affect journalists, even though legislative history makes it appear that Congress was unaware of this possibility and indeed did not want to prohibit the publication of defense information.

Sections 793(d) and 793(e) raise a host of complex issues. Who, for example, is entitled to receive defense information? One is tempted to think that this provision refers to the classification system that provides for authorized access after security clearance. The problem is that no such classification system existed in 1917, when the phrase in question was first used. Moreover, Congress until now has steadfastly refused to enforce the classification system with criminal sanctions. Another example: The phrase "relating to the national defense" here, unlike subsections 793(a) and 793(b), is not limited by a *scienter* (guilty intent) requirement and therefore may be subject to constitutional challenge on grounds of excessive vagueness and overbreadth. Similar problems arise in connection with the offense of retention. Given the constitutional rule that overly broad statutes touching on First Amendment freedoms may be attacked even by those whose activities could legitimately be subject to a narrower statutory regulation or prohibition, it is highly questionable that subsections 793(d) and 793(e) could survive judicial scrutiny if applied to the work of the press. The same result can be expected from the absence of a culpable intent requirement, generally necessary in statutes bearing on freedom of expression.

Exemption for the Fourth Estate

The conclusion that Congress in 1950 had not thought to enact a general prohibition on the publication of defense information is reinforced by its concurrent passage of section 798, which made it criminal to publish classified information concerning a narrow class of highly

secretive items, such as codes, ciphers, and cryptographic systems. Since those items clearly constitute "information relating to the national defense," it is reasonable to conclude—and the legislative history of section 798 supports this finding—that Congress did not consider the more general statutes an adequate protection against the publication of such information and therefore enacted more explicit legislation.

Other statutes bearing upon the publication of defense information for the most part aim at employees of the government. Here, too, it is apparent that Congress went out of its way to exempt newspapers and reporters from the reach of these laws. In 1933 Congress enacted what is now section 952 of Title 18 of the U.S. Code, which protects diplomatic codes. Enactment was prompted by the 1929 publication of a former State Department employee's book, *The American Black Chamber*, which described code-breaking procedures and included translations of decoded dispatches by the Japanese government. In late 1932 a second manuscript on the same subject was completed. The law that was approved punishes by fine or imprisonment anyone who "by virtue of his employment by the United States" obtains an official code or coded message and "willfully publishes or furnishes to another any such code or matter." A proposal to include anyone and not just present or former government employees was rejected. Debate over this bill made it clear that it was aimed solely at federal employees who breached their trust, not at reporters or newspapers publishing code material.

In 1950 Congress included in the Internal Security Act a provision that made it unlawful for an officer or employee of the federal government to communicate to any agent of a foreign government or member of an officially designated communist organization any classified information, "knowing and having reason to know that such information has been so classified." The provision is codified in section 783(b) of Title 50 of the U.S. Code; section 783(c) prohibits agents of foreign governments from knowingly receiving such classified information.

Foreign Agents

In the case of *Scarbeck v. United States*,[10] decided in 1962, the U.S. Court of Appeals for the District of Columbia upheld the conviction of a Foreign Service officer for communicating classified documents to representatives of the Polish government in violation of subsection 783(b). The argument of the defendant—that the jury should have passed on the propriety of the classification—was rejected. Unlike the espionage statutes discussed earlier, the so-called *Scarbeck* statute does not require the government to prove that the classified information related to the national defense or that it was communicated with intent to injure the United States or give advantage to a foreign government. The court made it clear that the *Scarbeck* statute covers only present officers or employees of the government, and it applies only when the recipient of the information was someone the defendant knew or had reason to believe was an agent of a foreign government or a member of a communist organization. In other words, a government employee who leaks classified information to a reporter has not violated the *Scarbeck* statute unless the reporter is a foreign agent or a member of a communist organization; an editor who publishes the information in his newspaper likewise has not committed an offense.

The Atomic Energy Act of 1946[11] includes a prohibition on the communication or disclosure of certain classes of "restricted data" concerning atomic weapons and nuclear energy—sections 2271–2281 of Title 42 of the U.S. Code. Section 2777 makes it unlawful for present or former government employees or contractors to disclose restricted data to anyone not authorized by the Atomic Energy Commission to receive same; the culpability standard in section 2774 covers not only willful infliction of injury on the United States or securing an advantage to a foreign nation but also recklessness, and perhaps negligence, in the handling of such data. Section 2275 makes criminal the receipt of restricted data with intent to injure the United States or advantage a foreign power.

The injunction proceeding that section 2280 authorizes against a violation was invoked in 1979, when Howard Moreland was writing a magazine article on the working of the hydrogen bomb. The government contended that the article contained restricted data. In March the U.S. District Court in Milwaukee issued a preliminary injunction prohibiting the *Progressive* from publishing the article and directing the author and editor to secure all copies.[12] This was the first time in U.S. history that a federal judge had imposed prior restraint on the press. However, before the injunction could be made permanent, several other newspapers, including the *Chicago Tribune*, published a letter by another author with similar technical data. In September, therefore, the Justice Department ended its efforts to prevent the publication of the Moreland article.

Sneak Previews

There is one other way in which the government can enforce secrecy: by exacting agreements from employees never to divulge without prior permission information related to the national defense that was acquired during the course of employment. Such secrecy agreements, used by the intelligence agencies, cover not only former agents but also the publishers of books written by such persons. In 1972 the government successfully relied upon a secrecy agreement to obtain an injunction requiring former CIA employee Victor Marchetti to submit his manuscript about the CIA for prepublication review.[13] As a result of this decision, left standing by the Supreme Court, Mr. Marchetti's book, *The C.I.A. and the Cult of Intelligence*, was published in 1974 with 168 deletions. A subsequent suit by Mr. Marchetti's publisher to use the deleted material ended in failure.[14]

Still another way to deter unauthorized publication of defense information is to seize the profits of books published in violation of a secrecy agreement. The government took this route when former CIA agent Frank Snepp published a book about the CIA's activities in South Vietnam without submitting it for review. The Supreme Court upheld the judgment against Mr. Snepp on the grounds that the former agent had willfully

breached his agreement with the CIA not to publish any information without clearance. "Whether Snepp violated his trust," the majority found, "does not depend upon whether his book actually contained classified information." The very fact that agents publish books about the CIA without approval weakens the agency's ability to perform its duties. Both foreign intelligence services and individual foreign agents increasingly question the advisability of working with a CIA that cannot guarantee the security of information likely to compromise them or endanger the personal safety of agents. The proper remedy, the Court concluded, was to enjoin future breaches of Snepp's agreement and to seize the profits of the book by way of a "constructive trust."[15]

All members of the Court ruling on the *Snepp* case agreed that even in the absence of a written contract, under the common law an employee has a fiduciary obligation to protect confidential information obtained during his employment and that a breach of this obligation could be punished by the seizure of personal profits from the exploitation of such information. This finding could open the way for the government to try to penalize any employee who publishes information about his official duties without first clearing it with his superiors. Guidelines issued in December 1980 by the outgoing attorney general of the Carter administration, Benjamin R. Civiletti, waived any intention to bring such suits unless there existed an express clearance obligation and unless the information was properly classifiable and likely to harm national security, but these were revoked by Attorney General William French Smith of the Reagan administration in September 1981.[16]

Foreign intelligence services . . . question . . . working with a CIA that cannot guarantee the security of information likely to compromise them . . .

On March 11, 1983, President Reagan issued National Security Decision Directive No. 84, "Safeguarding National Security Information," which requires all employees of the government with access to classified information to sign a nondisclosure agreement as a condition of access. Persons with access to Sensitive Compartmented Information (that is, highly sensitive intelligence information) from now on will also be required to sign a promise to submit all manuscripts for prepublication review. Such agreements are to be in a form enforceable in a civil action brought by the United States.[17] Whether the threat of civil suits will discourage leaks of confidential or classified information remains to be seen.[18]

A review of applicable law yields the conclusion that except for a narrow range of cryptographic information and restricted data concerning atomic energy, and except in cases where the sole purpose is communication to a foreign power, publication of defense information probably is not prohibited. Present or former employees of the government who in peacetime publish or leak such information to the press most likely are also not subject to any criminal sanctions other than possibly the seizure of profits gained. Until the prosecution of Daniel Ellsberg and Anthony Russo for their role in the publication of the Pentagon Papers, the government had never prosecuted any leak of defense information and had relied instead on administrative sanctions, such as dismissals, or the withdrawal of a security clearance. Despite numerous opportunities, no prosecution has ever been brought under the espionage laws for the publication of secret information damaging to national security. Even in the case of the Pentagon Papers, when an attempt to prevent publication was made, the government did not rely on the espionage statutes; some justices expressed the view that the espionage laws might have authorized criminal sanctions against the newspapers and reporters involved.

When in June 1971 the *New York Times* and the *Washington Post* began publication of the Pentagon's "History of U.S. Decision-Making Process on Viet Nam Policy," the so-called Pentagon Papers, the government went to court, arguing that the president's constitutional powers as commander-in-chief and steward of foreign relations entitled him to injunctive relief to prevent "grave and irreparable danger" to the public interest. Apparently, the government decided not to invoke the espionage statutes because it believed they did not authorize an injunction against publication. Yet this attempt to achieve equitable relief without regard to existing legislation failed. When the case reached the Supreme Court, the only proposition commanding a majority was that the government had not made an adequate record to justify the injunctive relief sought.[19] The basic question—whether publication of defense information violated espionage laws—therefore was untested.

Wartime, Peacetime

Of the ten opinions, Justice White's came closest to affirming the applicability of the espionage laws. The government, he argued, had not justified the imposition of prior restraint on publication, an action that under the First Amendment bears a heavy presumption against its constitutional validity. However, that the government had mistakenly chosen to proceed by injunction did not mean that it could not have successfully proceeded in another way. Various laws imposed criminal sanctions on the publication of certain types of defense information. "I would have no difficulty in sustaining convictions under these sections on facts that would not justify the intervention of equity and the imposition of a prior restraint."[20] Justice Stewart joined this opinion, and Chief Justice Burger registered "general agreement" with Justice White's view "with respect to penal sanctions concerning communication or retention of documents or information relating to the national defense."[21] Justice Blackmun, too, stated that he was "in substantial accord" with this position.[22]

Several justices also indicated that in some extreme cases they might even support the issuance of a restraining order to enjoin a newspaper from publishing sensitive

defense information in its possession. Quoting *Near v. Minnesota*, Justice Brennan affirmed that in times of war nobody would question the right of the government to prevent "the publication of the sailing dates of transports or the number and location of troops."[23] Justice White, joined by Justice Stewart, stated that by concurring in the decision of the Court, "I do not say that in no circumstances would the First Amendment permit an injunction against publishing information about government plans or operations."[24] Chief Justice Burger, too, rejected the view that the First Amendment asserts an absolute right of freedom of the press. Referring to the exceptions cited in *Near v. Minnesota*, he added: "There are no doubt other exceptions no one has had occasion to describe or discuss."[25] However, all of these comments represented *obiter dicta*—incidental remarks that did not provide a resolution of the important underlying question concerning the peacetime limits on the right of publishing national defense information.

The prosecution of Daniel Ellsberg and Anthony Russo might have resulted in some limited clarification of the espionage laws. Both men were indicted for violating subsection 793(e), which makes unlawful the unauthorized possession and retention of defense information. The principal event relied upon was the photocopying of the classified Pentagon Papers. Since to publish information, one must first possess it, a ruling on this indictment might have thrown some light on the legality of leaking—actions preparatory to publication. The men were also charged with stealing government property, though it was not clear whether the government regarded the information in the Pentagon Papers or the documents themselves as property. As it turned out, all these questions remained unanswered, since after the break-in at the office of Daniel Ellsberg's psychiatrist was discovered, the case was dismissed because of improper government conduct. The extent to which the leaking or publication of defense information constitutes a criminal offense under the espionage laws or other relevant statutes thus remains obscure.

Great Britain: Voluntary Compliance

The world's oldest democracy, Great Britain, has one of the most elaborate systems of official secrecy. This observation is not meant to suggest a causal connection between democracy and secrecy or to argue that the British tradition of secrecy is beyond criticism and should be copied. But although a democratic form of government requires that people be informed about basic issues of public policy, democracy does not rule out such measures as Britain's system of D (for defense) notices, which is designed to prevent sensitive information from falling into the hands of the country's adversaries.

The first British Official Secrets Act, passed in 1889, provided criminal sanctions against peacetime espionage and the unauthorized leaking or selling of information obtained by a civil servant. In 1911 this legislation was replaced by a new act that imposed penalties also on the recipient of unauthorized disclosures. Minor amendments were enacted in 1920 and 1939, but the important provisions are sections 1 and 2 of the 1911 act.

Section 1, concerned with espionage, is relatively uncontroversial except that it places on the accused the burden of proving that he did not act with a purpose prejudicial to the safety or interests of the state.

Section 2 makes it criminal for a civil servant or government contractor to communicate any kind of official information to an unauthorized person and for such a person to receive this information. "Official information" includes not only information related to national security but also any kind of data acquired in the course of employment. This section, it is generally agreed, is poorly drafted. It could lead to more than 2,000 differently worded charges, and it does not even fully clarify whether *mens rea* must be proven. The catchall provisions of the Official Secrets Act are saved from absurdity only by the requirement that prosecutions have the consent of the attorney general, and this consent has not often been given. Still, the many recipients of official information have little guidance for their day-to-day conduct of business. Moreover, the threat of prosecution puts a damper on the release of all kinds of information that cannot possibly be regarded as prejudicial to the state. Civil servants have been able to protect themselves from accusations of incompetence or mismanagement; debates on important issues have been handicapped by the public's lack of adequate background knowledge; discussion is constrained.

As Harold Wilson once put it: "It's easy to find the answers to the questions; what's difficult is to find the questions to the answers."[26]

Members of the press and the broadcasting services have the unofficial assurance that they will not be prosecuted for disclosing information concerning the national security as long as they comply with the D notices. These are issued to the newspapers and radio and television stations by the Defence, Press, and Broadcasting Committee, composed of four government officials from defense and national security departments and eleven representatives of the media. In urgent cases, the secretary of the committee, a full-time official of the Ministry of Defence, can issue a D notice on his own responsibility after obtaining the concurrence of two media members; indeed, the full committee rarely meets. The notices inform the media that the government regards a given item of information as secret and requests that it not be published.

Although compliance with the D-notice system is entirely voluntary, there have been few cases of nonobservance. The media have found it useful to have someone to consult on whether a proposed article might unintentionally harm an important national interest. During an official inquiry into the system in 1967, no media representatives suggested that it be abolished.[27]

Besides helping journalists and editors, the D-notice system undoubtedly enables them to minimize the ever-present threat of prosecution under the Official Secrets Act. Increased sensitivity to this threat, especially during the last fifteen years or so, has led to growing criticism of the act. In 1968 a committee concluded that the administrative process was surrounded by too much secrecy and recommended that the government examine the entire

subject of "unnecessary secrecy," including a review of the Official Secrets Act.[28] The Labour government of the day reacted defensively, but in 1970 the Conservative election manifesto promised to examine the operations of the act. In 1971 the new Conservative government appointed a committee under Lord Franks to review section 2 of the Official Secrets Act of 1911.

The report of the Franks Committee was published in September 1972. Its verdict: Section 2 was "a mess." People could not know what it meant or how it operated in practice or what kinds of action involved a risk of prosecution. The committee recommended that section 1 be replaced by an espionage act and section 2 by an official information act. The criminal sanctions of the act were to apply to four types of official information:

- Classified information relating to the defense or security of the realm or to foreign relations or the currency, the unauthorized disclosure of which was likely to cause serious injury to the interest of the nation. This category was to include information concerning the armed forces, weapons, military equipment, research and development of weapons or equipment, defense policy, military planning, the intelligence services, negotiations of treaties with other powers, and the like.
- Information likely to assist criminal activities or to impede law enforcement.
- Cabinet documents, so as to safeguard the collective responsibility of the cabinet.
- Documents entrusted to the government by a private individual or firm.

. . . close-up pictures of the gore of war on the nightly TV screens, for example, are not always conducive to winning.

The Franks report rejected the suggestion that the disclosure of classified information made in good faith and in the public interest was a valid defense against the charge of having caused serious injury to the nation. Damage to the national interest, it declared, does not depend on bad intentions. "It is caused when certain kinds of official information get into the wrong hands. It makes no difference whether the information reached those hands as a result of espionage or of leakage."[29] Before a prosecution for the disclosure of information, the appropriate minister should determine that the information was properly classified at least "Secret" or "Defense—Confidential." The idea of involving the courts in deciding the fact of injury to the nation was turned down. The leakage of other official information was to be dealt with through administrative, not criminal, sanctions.

The mere receipt of official information should no longer be an offense, the Franks report said, though further communication of classified information was to remain unlawful if done with awareness of the secret nature of the information. "If a civil servant has failed to protect a secret, there is no justification for the view that a citizen who thereby comes into possession of that secret, and who knows that it is a secret, should be free to compound the failure of the civil servant, and to harm the nation, by passing on the secret as he pleases."[30]

The proposals of the Franks Report were criticized as both too radical and too conservative. In the election campaign of 1974 the Labour party promised to replace the Official Secrets Act with a law that incorporated the principle of freedom of information. However, by the time the Labour government got around to making concrete proposals, pressure had grown for legislation that would establish a clear right to know. A bill incorporating this idea was introduced in 1978, but before Parliament could take final action, the government fell and Parliament was dissolved. A new proposal to replace section 2 of the Official Secrets Act was introduced in late 1979 with the backing of the new Conservative government. Critics called this bill worse than section 2 itself. But then Andrew Boyle's *Climate of Treason* was published. It led to the revelation that Sir Anthony Blunt, former keeper of the Queen's pictures, was once a Soviet agent. Under the government bill, it was now pointed out, the publication of that book and all public discussion of the Blunt case would have been a criminal offense. The government thereupon withdrew its bill, and no new legislative initiative has had its backing since then.

The Official Secrets Act thus remains British law. As one critic of Britain's continuing tradition of government secrecy has put it: "Britain is about as secretive as a state can be and still qualify as a democracy."[31]

After the conclusion of the Falklands conflict in 1982, several well-known British journalists complained about censorship. Others have argued that there are some things more important than the people's right to know and that close-up pictures of the gore of war on the nightly TV screens, for example, are not always conducive to winning. "We British," a lead writer for the *Daily Telegraph* has observed, "practise the residual secrecy of an old empire linked up with the new bureaucratic style of a country enmeshed in civil servants. It isn't something to be idealistic about, but arguably it makes the courage of soldiers and the will of a strong Prime Minister just that degree more likely to achieve their ends and gives them a breathing space in which to do what is necessary."[32]

Sweden: Certain Sanctions

Sweden is another democratic country that insists on preventing the publication of certain types of defense information. A tradition of open government was established by the Freedom of the Press Act of 1766, which is part of Sweden's constitution. Under this law, amended in 1937, all government papers, unless specifically exempted by the act, are open for public inspection. A system of appeal and review is available when access is denied. The law also incorporates the Secrecy Act, which provides criminal sanctions for the publication of matters concerning foreign policy or defense that if disclosed could threaten national security. Furthermore, the es-

pionage section of the penal code authorizes the prosecution of anyone "who, with the intent of aiding a foreign power, without authorization, obtains, transmits, gives, or otherwise reveals information . . . the disclosure of which to a foreign power can bring harm to the defense of the Realm." This law also applies to a person who, with like intent, "without authorization produces or is concerned with a writing, drawing or other object containing such information."[33]

The seriousness that Sweden attaches to protecting information was apparent in the so-called IB affair in 1973. Helped by leaks from a civil servant, two left-wing journalists that year prepared and published a series of articles about the Swedish Information Bureau. The articles gave the names of IB officials, the addresses of IB offices, and information about cooperation between the IB and the security services of other countries, such as the United States, Great Britain, and Israel. Contrary to expectations, the informant and the two journalists were charged not under the Secrecy Act but under the espionage law. They were tried *in camera* and sentenced to jail terms; a court of appeal affirmed that they had acted with an implied intent to aid a foreign power within the meaning of the espionage statute.[34]

The verdicts in the IB affair drew considerable criticism. A commission of inquiry was appointed to consider changes in the Freedom of the Press Act. The revised law, which came into force in 1978, makes all prosecution of the press a matter to be decided by the attorney general. In 1981 a new secrecy act went into effect; it expands the scope of secrecy and tightens the law with regard to unauthorized leaks by civil servants.

West Germany: Militant Democracy

A third democracy that has wrestled with the problem of reconciling freedom of the press and protection of state secrets is the Federal Republic of Germany. Article 5(1) of West Germany's constitution, the *Grundgesetz*, or basic law, affirms the right of the people to unhindered information, freedom of speech, and freedom of the press, and it rules out censorship. But public speech, like all rights of the person, can be limited by general laws that seek to protect the public interest. The importance attached to the defense of the democratic order is manifested by West Germany's commitment to the principle of "militant democracy." Unlike the Weimar Republic, which is held to have succumbed in part because its opponents were able to use their civil rights to destroy the democratic constitution, West Germany asserts the authority to deny freedom to the enemies of freedom. The principle of militant democracy does not directly touch upon the protection of official secrets, but it is a significant aspect of West Germany's political culture.

According to section 61 of the civil service law, civil servants are required to keep secret all information acquired in the course of their official duties. A violation of this provision is punishable with up to five years' imprisonment. However, this sanction can be invoked only if the information involved jeopardizes important public interests. A similar qualification is attached to the definition of state secrets—"facts, objects or knowledge that are accessible only to a limited number of persons and that must be kept secret from a foreign power in order to avert the danger of serious damage to the external security of the Federal Republic of Germany." The disclosure of such a secret is a criminal offense if the offender reveals it to a foreign power, allows it to get into the hands of unauthorized persons, or publishes it to disadvantage the nation or favor a foreign power. Again, the disclosure is punishable only if it creates a danger of serious damage to the external security of the country. Moreover, the civil servant incurs neither disciplinary nor criminal liability if after exhausting all other remedies, such as informing his superiors or his representative in the legislature, he reveals information concerning unconstitutional activities of his government—activities that undermine the democratic order or violate treaty-imposed restrictions on German armaments.[35] Presumably, this provision would also protect whistle-blowing on preparations for a war of aggression, forbidden by the basic law, even though in the age of preemptive wars it may not be easy to determine whether an attack on another country constituted aggressive warfare.

Until 1968 the law concerning treason did not distinguish between the intentional betrayal committed by the agent of a foreign power and the disclosure of a state secret by a journalist. The need for such a distinction was driven home by the *Spiegel* affair, which rocked West Germany in October 1962. In an unprecedented legal maneuver, the publisher and several leading editors of the mass-circulation magazine *Der Spiegel* were arrested for publishing an article on the state of readiness of the German armed forces. The article, it was alleged, made use of classified information, and the persons responsible for its publication were therefore to be charged with the crime of treason. Following an outcry of protest all over the country, this proceeding was aborted. A member of the Bundestag who was suspected of having given *Der Spiegel* a classified document could have been charged with violating Section 353c of the criminal code, but this indictment, too, was never pressed.

Section 353c was abolished in 1979. Journalists had referred to it as the "muzzle paragraph," since it provided a prison term of three years or a fine for anyone who communicated or published classified information and thereby endangered important public interests. A violation, critics pointed out, was triggered by the very fact of publishing classified information, whether or not the information was properly classified or even involved an important secret. Now modified, the law would reach a journalist only if he published a classified document given to him by a civil servant and if he had been formally informed of his obligation to keep it secret.

Prosecutions under the old law had been extremely rare; they are even less likely under the new.[36] Moreover, a journalist could still plead that the information, although classified, concerned an important aspect of public life and that its disclosure therefore was justified on account of the constitutionally guaranteed right of citizens to be informed—as well as by the guarantees of freedom of speech and press. That was the clear implication of a supreme court ruling in the aftermath of the

Spiegel affair. It is generally recognized that a judge who had to weigh the relative importance of these rival public goods in order to decide the justification of "journalistic treason" would face an extremely difficult and delicate task.[37] To what extent, for example, could an article on the stationing of middle-range missiles in West Germany go into details about the location, reach, and power of such missiles? How much technical, possibly classified, detail does a journalist need to write intelligently about these complex and yet highly important issues of foreign and military policy so that people can form opinions about them? At what point does a public discussion of military strategy and tactics in the age of atomic weapons aid a foreign power, if only by demoralization from harping on the disastrous consequences of a nuclear exchange? These questions, of importance for other countries besides West Germany, await answers.

". . . when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless . . ."

Several facts of American political life greatly complicate matters. There is, first, the ever-present problem of overclassification. The basic need to withhold from the public certain kinds of information is generally accepted. It is elementary, Justice Stewart pointed out in the Pentagon Papers decision, "that the successful conduct of international diplomacy and the maintenance of an effective national defense require both confidentiality and secrecy. Other nations can hardly deal with this Nation in an atmosphere of mutual trust unless they can be assured that their confidences will be kept. And within our executive departments, the development of considered and intelligent international policies would be impossible if those charged with their formulation could not communicate with each other freely, frankly, and in confidence. In the area of basic national defense the frequent need for absolute secrecy is, of course, self-evident."[38] Yet secrecy has often become an end in itself.

Ever since the beginning of the modern security classification system in World War I, bureaucrats have tended to play it safe and overclassify, prolonging the period of restriction and placing roadblocks in the way of access. Some experts—former high officials of the executive branch—who have testified about this problem before the Congress have estimated that as much as 75 percent of the documents now classified do not require protection against disclosure.[39] Such abuse undermines the credibility of the entire program. To quote Justice Stewart again: "For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion."[40]

A system of classification that lacks integrity is a direct cause of leaks. Government employees, frustrated by the amount of secrecy under which they have to operate, feel justified in leaking or otherwise compromising classified information. The leaking of the Pentagon Papers to the press by Daniel Ellsberg is the best-known example of such a breach of trust, but there have been numerous other cases where government employees decided to disclose important defense or diplomatic information. Was the information really in need of classification? Did these disclosures help create a more enlightened citizenry, better equipped to judge issues of public policy and select public officials? These questions are probably somewhat beside the point. Apart from the exposure of manifest corruption or illegality, it is difficult to run an orderly government if each employee can function as the public conscience and take upon himself the right to disregard the rules. Individual employees may not know why secrecy is important. All too often such disclosures, even those made with the best of motives, have ruled out a foreign policy option or jeopardized ongoing policy.

The problem of preventing or tracking down leaks of classified information by low-level government employees is extremely difficult. Another complicating element is the widespread practice by top officials of declassifying information they want to leak. These authorized leaks take several forms. The most frequent technique is the off-the-record press briefing or "backgrounder," which is filtered to the public under the rubric "according to informed sources." The purpose may be to float a trial balloon, testing public reaction, or to justify a certain policy or fortify one's position against a rival bureaucrat. High officials can also disclose confidential or classified information in memoirs published after they leave office. All of this leads to charges of a double standard and further weakens confidence in the integrity of the classification system. As one critic has put it, probably with only slight exaggeration: "Authorized leaking makes a mockery of information law because policy-makers enforce arbitrary criteria against others while being themselves engaged in systematically releasing self-serving news on a not-for-attribution basis."[41]

Briefing or Leaking?

Some officials draw a distinction between briefing the media (a good thing) and leaking to the media (a bad thing). Others honestly acknowledge the difficulty of such a differentiation. "You know the difference between leaking and briefing," James Callaghan, Labour's Home Secretary, once said. "Briefing is what I do, and leaking is what you do."[42] One can also argue that when a high-level official engages in instant declassification, he is merely doing that to which he is entitled by law, for the authority to classify includes the right to declassify. But such officials should have some perspective on the results of such disclosures.

Several attempts to put a criminal sanction on the communication or publication of classified defense information have ended in failure. In 1957 the Commission on Government Security recommended "that Congress enact legislation making it a crime for any person willfully

to disclose without proper authorization, for any purpose whatever, information classified 'secret' or 'top secret,' knowing, or having reasonable grounds to believe, such information to have been so classified."[43] A bill that did not require a specific intent to injure the United States was introduced but failed to win much political support. Similar proposals were advanced during the attempted recodification and revision of the federal criminal code in 1973. One of these bills, S.1, made the publication of national defense information explicitly criminal only in time of war. The proposal of the Nixon administration, S.1400, was more sweeping and, as critics contended, would have paralyzed most newspaper reporting on national security affairs.[44] Prolonged efforts to work out an acceptable compromise failed, and the federal criminal code reform bill finally died in 1982.

Poking through the Files

The Watergate scandal and the attendant abuses in the name of national security have undoubtedly created great difficulties for the enactment of legislation to protect the nation's security interests. Passage of even a modest proposal—the law to protect the identities of U.S. intelligence agents—required the expenditure of a lot of political capital. The United States today denies its intelligence agencies the secrecy granted to physicians, lawyers, clergymen, grand juries, and income tax returns; it is the only country in the world that gives foreign intelligence agencies, not to mention anyone else, a legal license to poke into the files of its intelligence organizations. The willingness of our allies' intelligence services to share their information and the willingness of individuals to risk their lives and reputations to help us have seriously diminished, yet bills to exempt the intelligence agencies from the coverage of the Freedom of Information Act have made no headway. The public has developed a right-to-know mentality, and journalists consider any information, no matter how sensitive, fair game. Nevertheless, it would be the course of political prudence to consider and take action on the thorny problem of protecting national defense secrets in a period of relative domestic calm—before a major disaster whips up hysteria and leads to an overreaction.

Two types of conduct that are potentially damaging to national security are not explicitly covered by existing law. The first is the unauthorized disclosure by present or former government employees of classified defense information acquired during the course of their employment. Such disclosure is now criminal only if made to an agent of a foreign power or a member of a communist organization or if it involves a narrow range of cryptographic information or data concerning atomic energy. The espionage statutes that prohibit the disclosure of national defense information to anyone not authorized to receive it lack a *scienter* requirement and generally are so broadly phrased that they are unlikely to pass the test of constitutionality.

A new, more comprehensive statute aimed at the unauthorized disclosure by government employees of defense information should encompass all information properly classified secret or top secret. Those charged with violating such a law should be able to challenge in court the propriety of classification. However, this review should not be *de novo* but should be limited to a determination by the judge that the government, acting through an authorized official, had correctly applied its own rules concerning the protection of sensitive defense information. The judge might also be given the right, as in West German law, to quash prosecution if the classified information concerned illegal activities.

Until 1980 the government often hesitated to press such prosecutions lest defendants, invoking the discovery and other rights under the federal rules of criminal procedure, obtain additional sensitive material and disclose it in the courtroom, thereby compounding the injury done national security by confirming the information's authenticity and significance. Prosecutors viewed this tactic as similar to blackmail because it left them the choice of augmenting the initial damage or abandoning prosecution. This "graymail" problem was largely solved by the enactment of the Classified Information Procedures Act in October 1980.[45] Under this law, a judge can hold *in camera* pretrial hearings on the use of classified information, and he can prevent the disclosure of classified data given the defendant by the government.

It would probably be unwise, as some have suggested, to grant judges the unfettered discretion to decide whether the information, though properly classified, concerned an important aspect of public life and had such significance for public debate that its disclosure was in the national interest. Judges have traditionally shied away from encroaching on the executive's control over foreign and military policy, and this reluctance appears especially justified when the issue is the determination of a disclosure's probable impact on the nation's security. Such determinations, like all executive decisions concerning foreign policy, Chief Justice Burger correctly pointed out in the Pentagon Papers case, "are delicate, complex, and involve large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry."[46] A test of the factual basis of the executive's claim of risk or damage would involve a vast and complicated area of facts and contingencies relating to foreign policy that the judiciary cannot be expected to master.

Chronic Overclassification

A statute criminalizing government employees' unauthorized disclosure of classified defense information will be workable only if the executive branch makes substantial progress in controlling the chronic problem of overclassification. Then it will be possible to argue that the revelation of secret or top-secret defense information constitutes the kind of damage to the security of the nation that justifies criminal penalties. To safeguard against frivolous prosecution, both the secretary of the department concerned and the attorney general should be required to authorize prosecution. Finally, to answer

the charge of selective law enforcement, public officials will have to restrain their habit of engaging in instant declassification. All this, undoubtedly, is a tall order and will require considerable change in current practice. However, the harm caused by certain kinds of leaks, currently left unpunished, is great enough to call for some special efforts. Moreover, failure to protect secrecy can result, paradoxically, in an increase in secrecy: "If the legal order legitimates the view that respect for secrecy is only a matter of political commitment, the likely response of the decision-makers will be to make secrets available to only a few trusted subordinates. Thus, the law's failure to give weight to security considerations will augment the tendency to centralize power into fewer hands."[47]

The second type of conduct that should be covered by new law is the publication of leaked national defense information. Currently, the only publication that is clearly prohibited aims specifically at informing the enemy in time of war, or has the main purpose of identifying intelligence agents, or concerns codes, a narrow class of cryptographic information, and restricted data on atomic energy. The press in a democratic society plays an extremely important role in informing the public and lawmakers about public policy, a role as essential in matters of foreign policy as in other areas of national life. And yet our society also has a clear need to protect the secrecy of certain types of defense information. Should the press be entitled to disregard this need once it has managed to get hold of such sensitive information? The answer that Britain's Franks Committee fashioned bears repeating: "If a civil servant has failed to protect a secret, there is no justification for the view that a citizen who thereby comes into possession of that secret, and who knows that it is a secret, should be free to compound the failure of the civil servant, and to harm the nation, by passing on the secret as he pleases." Journalists, too, are citizens; they should have the same obligations.

. . . most segments of the media today treat as a scoop any information, no matter how sensitive, that comes their way.

Accepting this view in principle, Professors Edgar and Schmidt have suggested that Congress set strict limits to prohibitions of unauthorized disclosure and publication of national defense information. "Only very narrowly drawn categories of defense information of great security significance and, in most cases, little import for public debate, should be prohibited from public revelation. Information about cryptographic techniques, intelligence-gathering operations, the design of secret and vital weapons systems, nuclear armaments, and perhaps other narrow and concrete categories of defense or intelligence information are appropriate subjects, in our opinion, for prohibitions on peacetime press disclosure."[48] But could Congress formulate an adequate catalogue of protected defense information? Is Congress any better equipped than the judiciary to foresee the possible harm that could come from the publication of certain kinds of secrets? Could Congress make a list of prohibited items that would enable journalists, prosecutors, judges, and juries to know with certainty what may not be published? The danger is that any such list would be either too specific and therefore lacking in flexibility or so general that it left considerable ambiguity of interpretation.

Defenders of the press point to the Bay of Pigs episode in 1961 as the kind of case where the press should have gone ahead and published whatever it knew to prevent a disastrous policy failure. More recently, the press has published details about CIA covert operations in Central America, especially against Nicaragua. Presumably, the journalists and editors responsible for these articles felt entitled to publicize these operations because they questioned their wisdom. Information about this covert effort is said to have come from intelligence officials and apparently also from those in the Congress, the Defense Department, and the State Department who are worried about the CIA's role in Central America. "Some officials fear," the *New York Times* wrote in December 1982, "that the activities may aggravate chronic political instability in the region and lead to eventual direct military involvement there."[49] It is possible that the CIA deliberately revealed information about these covert operations to exert pressure against Nicaragua. On the other hand, some of the information may have been leaked by people in the Reagan administration who are critical of this policy. If the latter, should the press be free to compound the impact of a lack of cohesion among decision makers by publicizing the leaked information? Does the importance of public debate on this issue justify disclosure of validly classified information? Who should decide?

Permanent Adversaries

The problems raised would be less serious if one could be sure that the media were prepared to assume responsibility for protecting legitimate needs of national security. Unfortunately, this assumption is not universally valid. The United States was able to fight World War II without compulsory censorship, but the consensus on goals between government and press that made this possible no longer exists. The willingness of the media to publish leaks about such delicate issues as the Glomar Explorer mission to lift a sunken Russian submarine or U.S. relations with Pakistan and Jordan in several recent crises indicates that most segments of the media today treat as a scoop any information, no matter how sensitive, that comes their way. They are no longer merely occasional critics of government but permanent adversaries. Whatever little restraint national newspapers like the *New York Times* or the *Washington Post* are still prepared to practice cannot be expected from papers like *Ramparts*, the *Madison Press Connection*, or the *Daily Californian*, all of which question the very need for national secrets.

The difficulty of obtaining the voluntary cooperation of the press in protecting sensitive defense information

was illustrated by a recent episode in Washington. On December 14, 1982, the Defense Department scheduled a special press briefing about Soviet military capabilities. The briefing was designed to convince reporters that the government had solid evidence of the grave military threat to the United States and its allies in Europe posed by the Soviet Union's growing military might. The thirteen reporters present were asked to sign a secrecy agreement, but none were willing to do so. The original intent, it appears, had been to protect merely the sources of the information—photographs taken by high-flying American reconnaissance aircraft or satellites, for example—but the wording of the agreement that was in fact given to the reporters was more sweeping and would have prohibited all dissemination of the information. For the *New York Times*, apparently, any kind of restraint was unacceptable. The paper declined to send a correspondent to the briefing; its managing editor, Seymour Topping, explained the decision by saying, "The *Times* does not enter agreements that bar a reporter from sharing information with readers or responsible editors."[50]

To create a new political climate regarding the treatment by the press of U.S. foreign and military policy, I favor legislation prohibiting the publication of defense information classified secret or top secret. The media should be vigorous in airing general issues of policy, but they should not presume to judge what kind of data require protection against disclosure. That decision must be made by those responsible and accountable for foreign policy, and their judgment, unless patently arbitrary, should be binding. The only exceptions to this rule should be those mentioned earlier in connection with the disclosure of classified information by present or former government employees. Recourse to prior restraint by an injunction against publication should be limited to situations of reckless disregard of serious injury to the national security, certified as "journalistic treason" by a committee of experts. Such a committee, to be appointed in equal parts by the Congress and the president, should be composed of distinguished former foreign policy, defense, and intelligence officials with full access to classified information. Their recommendations would not be legally binding, but they would help judges determine the likely consequences of a breach of secrecy.[51] There is reason to believe that such legislation would not conflict with the First Amendment, which does not require an unlimited right of public speech and publication.

There is also the problem of unclassified technical and scientific data of potential military value to the Soviet Union and other foreign nations. Defense and intelligence officials have warned that the Soviets for some time have conducted a highly orchestrated effort to gather technical information to enhance their military capabilities. The problem here again is to avoid all-or-nothing approaches. The unfettered exchange of ideas is an important element in the scientific edge that this country enjoys over the Soviet Union in most fields of study; a continuation of that freedom of communication in scientific research is essential to further progress. However, some screening of publications dealing with devices and technical plans that can quickly be applied to military or industrial use is perhaps indicated. It might be possible to use the British D-notice system or to develop a modified version of the voluntary system of control that functioned so well in this country during World War II. Beginning in 1941, the government issued the Code of Wartime Practices, which identified information that might be helpful to the enemy and should not be published without prior consultation. Compliance with this system was voluntary, yet there were no instances of intentional violation. The major factor in the success of this program apparently was that it was operated in a manner that won the respect of the press.[52] Could the scientific community today be persuaded to muster a similar spirit of cooperation and accept the need for some curb on the free flow of unclassified scientific information? That is an open question.

Legal systems work when the law is perceived as fair, just, and necessary. In the final analysis, therefore, the actual results of the legislation proposed here will depend on basic political attitudes and shared values that can be influenced by law—and most men respect that which is legal. But the results will also depend on nonlegal factors. Britain's D-notice system works because there exists a reservoir of basic trust between government and the governed, including the media. Whether such a consensus on common national aims can be restored in the United States will have as much significance for the better protection of the nation's secrets as the enactment of new legislation.

References

1. 40 Stat. 217 (1917).
2. 64 Stat. 1003 (1950).
3. For a careful analysis of the legislative background of sections 794(a) and 794(b), see Harold Edgar and Benno C. Schmidt, Jr., "The Espionage Statutes and Publication of Defense Information" in *Columbia Law Review*, LXXIII (1973), pp. 991–998. My discussion of the espionage statutes draws extensively on this excellent study. For a shorter and less technical version of this monograph, see Benno C. Schmidt, Jr., "The American Espionage Statutes and Publication of Defense Information" in *Secrecy and Foreign Policy*, edited by Thomas M. Franck and Edward Weissband (New York, 1974), pp. 179–201.
4. Some publications, such as *Counter Spy*, may have as their aim the infliction of damage on U.S. foreign policy, but section 794(b) will not reach them except, at best, in time of war. Whether it would be possible to prove the requisite intent to aid the enemy or whether the presence of other intents, such as informing the public, would be exculpatory is an open question. To prevent these kinds of complications, section 301(c) of the Intelligence Identities Protection Act of 1982 (Public Law 97-200, 96 Stat. 122, 50 U.S.C. 421) uses in place of the intent standard a supposedly more objective standard requiring that the disclosure be "in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such

activities would impair or impede the foreign intelligence activities of the United States."

5. 312 U.S. 19 (1941).
6. Ibid., pp. 28–29. Among the factors to be considered, another court ruled in 1962, is whether the information involved is classified. *United States v. Soblen*, 301 F.2d 236 (2d Cir.), cert. denied, 370 U.S. 944 (1962). But how important should the mere fact of classification be in establishing that the information concerned the national defense? Should the jury regard only information *properly* classified as defense related?
7. 151 F.2d 813 (2d Cir. 1945), cert. denied, 328 U.S. 833 (1946).
8. *Gorin v. United States*, 312 U.S. 19, 27 (1941).
9. A reading of the culpability standard that stresses what the obtainer of the information thinks will be its principal use would reconcile the broad language of the statute with what we know about Congress's objection to a blanket prohibition on publication. An opinion issued in 1942 by Attorney General Francis Biddle held the transfer of defense information to our European allies under the Lend-Lease program not to constitute a violation of the espionage statutes: "Under the circumstances here involved, the primary advantage sought is that of the United States itself; the conferring of an advantage upon an allied nation is but a means to that end." 40 Opinions of the Attorney General 250 (1942), cited by Edgar and Schmidt, *op. cit.*, p. 998.
10. 317 F.2d 546 (D.C. Cir. 1962), cert. denied, 374 U.S. 856 (1963).
11. 60 Stat. 766 (1946), as amended 68 Stat. 958 (1954).
12. *United States v. The Progressive*, 467 F. Supp. 990 (1979).
13. *United States v. Marchetti*, 466 F.2d 1309 (4th Cir. 1972), cert. denied, 409 U.S. 1063 (1972).
14. *Knopf v. Colby*, 509 F.2d 1362 (4th Cir. 1975).
15. *Snepp v. United States*, 444 U.S. 507 (1980).
16. Cf. A. O. Sulzberger, Jr., "Guidelines Laid Out on Secrecy Breaks" in the *New York Times*, December 4, 1980; Mary Thornton, "Reagan Tightening the Rules on Leaking" in the *Washington Post*, September 17, 1981.
17. Robert Pear, "President Orders Curb on Handling of Classified Data" in the *New York Times*, March 12, 1983.
18. For a discussion of the rationale of the new presidential directive, see Daniel B. Silver, "Safeguarding National Security: A Defense of Reagan's Directive," *Intelligence Report*, Vol. V, No. 6 (June 1983), pp. 1–2.
19. *New York Times Company v. United States*, 403 U.S. 713 (1971).
20. Ibid., p. 737.
21. Ibid., p. 752.
22. Ibid., p. 759.
23. Ibid., p. 726, citing *Near v. Minnesota*, 283 U.S. 697, 716 (1931).
24. Ibid., p. 731.
25. Ibid., p. 749.
26. Quoted in Anthony Sampson, "Secrecy, News Management, and the British Press" in Franck and Weissband, *op. cit.*, p. 224.
27. Ibid., p. 225. On the D-notice system, see also James Michael, *The Politics of Secrecy* (Harmondsworth, 1982), pp. 86–90.
28. Great Britain, *The Civil Service: Report of the Committee* (Lord Fulton, chairman), Cmnd. 3638 (1968).
29. Great Britain, Home Office, *Report of the Departmental Committee on Section 2 of the Official Secrets Act 1911, Lord Franks*, Cmnd. 5104 (1972), Vol. I, p. 40.
30. Ibid., p. 85.
31. Michael, *op. cit.*, p. 9.
32. Edward Pearce, "Old Strengths, Discovered Anew: After the Falklands," *Encounter* (September–October 1982), p. 38.
33. Quoted in Michael, *op. cit.*, p. 151.
34. Ibid., pp. 149–152.
35. This was the holding of the Federal Constitutional Court in 1970. See M. M. Bullinger, "Western Germany" in *Administrative Secrecy in Developed Countries*, edited by Donald C. Rowat (New York, 1979), p. 233.
36. Cf. Manfred Möhrenschlager, "Das siebzehnte Strafrechtsänderungsgesetz," *Juristenzeitung*, XXXV (1980), 165. See Heinrich Laufhütter, "Staatsgeheimnis und Regierungsgeheimnis" in *Goltdammer's Archiv für Strafrecht*, LII (1974), pp. 52–60.
37. Cf. Peter Lerche, "Geheimschutz und Öffentlichkeitsinteresse" in Bundesministerium des Innern, comp., *Verfassungsschutz und Rechtsstaat* (Cologne, 1981), pp. 117–132.
38. *New York Times Company v. United States*, 403 U.S. 713, 728 (1971).
39. See the essay by Representative William S. Moorhead of the House Committee on Government Operations, "Operation and Reform of the Classification System in the United States" in Franck and Weissband, *op. cit.*, pp. 87–113.
40. *New York Times Company v. United States*, 403 U.S. 713, 729 (1971).
41. Alan M. Katz, "Government Information Leaks and the First Amendment," *California Law Review*, LXIV (1976), p. 110.
42. Cited by Stanley de Smith, "Official Secrecy and External Relations in Britain: The Law and Its Context" in Franck and Weissband, *op. cit.*, p. 318.
43. *Report of the Commission on Government Security* (Washington, D.C., 1957), p. 620.
44. Cf. Edgar and Schmidt, *op. cit.*, pp. 1079–1083.
45. Public Law 96–456, October 15, 1980, 94 Stat. 2025, 18 U.S.C. Appendix 84.
46. *Chicago and Southern Air Lines v. Waterman Steamship Corporation*, 333 U.S. 103, 111 (1948), cited by Justice Burger in *New York Times Company v. United States*, 403 U.S. 713, 758 (1971).
47. U.S. Congress, Subcommittee on Legislation of the House Permanent Select Committee on Intelligence, *Espionage Laws and Leaks*. 96th Congress, 1st sess., hearing, January 25, 1979, p. 114.
48. *Loc. cit.*
49. See, e.g., Philip Taubman, "C.I.A. Is Making a Special Target of Latin Region" in the *New York Times*, December 4, 1982.
50. Philip Taubman, "Reporters Balk at Secrecy Pledge" in the *New York Times*, December 15, 1982.
51. For an illuminating discussion of this suggestion in a German context, see Gerd Ruge, ed., *Landesverrat und Pressefreiheit: Ein Protokoll* (Cologne, 1963), pp. 113–114.
52. Cf. "Developments in the Law: The National Security Interest and Civil Liberties," *Harvard Law Review*, LXXXV (1972), p. 1194.